

**Amendments to the Claims**

This listing of claims will replace all prior version, and listings, of claims in the application:

**Listing of Claims:**

1.-4. (CANCELLED)

5. (CURRENTLY AMENDED) A process for securing information in a digital form comprising: creating an identifier using information obtained from a device capable of rendering the digitized information to be secured;

associating the identifier with the information to be rendered;  
securing said digitized information by preventing the rendering of the information if the identity of the device upon which the information is to be rendered is not verified using said identifier,

wherein the identifier is a binary key suitable for use in an algorithm that can secure said digitized information~~The process as set forth in claim 2,~~ and wherein the information associated with the specific physical device that is to be used to render the secured information is produced by:

- obtaining information representing a physical or functional attribute of at least one component in said physical device which is unique to that component; and
- converting said information into a binary key by performing a cyclic redundancy check or other repeatable process on said information.

6. (CANCELLED)

7. (CURRENTLY AMENDED) A process according to claim 5, wherein the identifier comprises a binary key of at least 64 bits in length and wherein the information is secured by preventing the rendering of the information by the device on the basis of information produced by a test for authentication of the device using the said binary key and an algorithm suitable for authentication. 7. A process according to claim 6, wherein the information is secured by preventing the rendering of the information by the device on the basis of information produced by a test for authentication of the device using the said binary key and an algorithm suitable for authentication.

8. (CURRENTLY AMENDED) A process according to claim 5, wherein the identifier comprises a binary key of at least 64 bits in length and wherein the information is secured by preventing the operation of the device on the basis of information produced by a test for authentication of the device using the said binary key and an algorithm suitable for authentication. 8. A process according to claim 6, wherein the information is secured by preventing the operation of the device on the basis of information produced by a test for authentication of the device using the said binary key and an algorithm suitable for authentication.

9. (ORIGINAL) The process as set forth in claim 7 wherein the test for authentication comprises comparing information associated with the data to be rendered with information produced by an evaluation of the device which is to be used to render said data.

10. (ORIGINAL) The process as set forth in claim 9 wherein the evaluation of the device occurs during the process of authentication.

11. (ORIGINAL) The process as set forth in claim 9 wherein the information to be rendered is received by the device in an encoded format, and is unencoded prior to rendering by said device.

12. (ORIGINAL) The process as set forth in claim 9 wherein the information to be rendered is received by the device in an encoded format distinct from a format that the device can use to render said information, and said information is unencoded prior to rendering by said device.

13. (ORIGINAL) The process as set forth in claim 9 wherein the information to be rendered is received by the device in a format the device can render without subsequent transformation.

14. (CURRENTLY AMENDED) The process as set forth in claim 9~~claim 6~~ wherein the physical device is a general purpose computer and the component is selected from the group consisting of a bus, a microprocessor, an integrated circuit, a hard drive; a video display circuit, a network interface circuit, a video display card, a network interface card or a circuit located on a peripheral connected to a local bus on said system.

15.-21. (CANCELLED)

22. (CURRENTLY AMENDED) The process as set forth in claim 5-claim 15, wherein the process further comprises:

- segmenting the data to be distributed into one or more blocks;
- defining an arbitrary numeric or alphanumeric indicator representing the level of security employed by the distribution process;
- producing a data size indicator representing at least the size of the block of data;
- producing an encoded data content indicator representing the unsegmented encoded information;
- producing an encoded checksum by performing a cyclic redundancy check operation on the file containing the encoded information;
- producing a block integrity verifier by performing a cyclic redundancy check operation on a file comprising the security indicator, the size indicator, the encoded data content indicator and the encoded checksum; and
- combining the security indicator, the size indicator, the encoded data content indicator, the encoded checksum and the block integrity verifier.

23.-24. (CANCELLED)

25. (CURRENTLY AMENDED) The process as set forth in claim 22-claim 24, wherein the information is secured by preventing the reading of data from the medium containing the software to be installed.

26. (CANCELLED)

27. (CURRENTLY AMENDED) The process as set forth in claim 25-claim 26, wherein the medium is a floppy disk and the alteration is effected by permanently altering sectors of the disk to encode on said disk the pre-defined arbitrary identifier.

28. (ORIGINAL) The process as set forth in claim 27, wherein the permanent alteration of said disk is effected by physically altering magnetic oxide residues on said disk which do not correspond to recorded bits on said disk.

29. (ORIGINAL) The process as set forth in claim 28, wherein said permanent alteration is effected by using a laser to destroy said magnetic oxide residues.

30. (ORIGINAL) A process of installing software across a network in a manner that prevents the unauthorized duplication or use of the software after it has been installed on a specific computer comprising:

- initiating an installation process for installing software onto a computer from a server computer using a network;
- producing a unique identifier using information derived from at least one physical component of the computer upon which the software is to be installed;
- including the unique identifier in at least one file associated with the software to be installed, wherein the absence of said file prevents operation of the software;
- transferring the files including at least the said file containing the included identifier to the computer upon which the software is to be installed;
- at the time of execution of the software after it has been installed,
  - producing a unique identifier using information derived from at least one physical component of the computer upon which the software is to be installed;
  - comparing the unique identifier to the unique identifier embedded in the said at least one file associated with the software;
  - if the comparison provides a pre-defined negative result based on the unique identifiers, preventing the software from executing, preventing the operation of the software.

31.-42. (CANCELLED)

43. (ORIGINAL) A process for securely distributing information representing an audio or audiovisual work comprising:

- producing a binary key using information derived from at least one physical component of a device capable of rendering the work;
- associating with the information representing the audio or audiovisual work the binary key produced;
- distributing the information to the location at which the information is to be rendered;
- prior to or during the rendering of the information on a device capable of rendering said information,
  - producing a binary key using information derived from at least one physical component of the device;
  - retrieving from said information the binary key associated with said information;
  - comparing the binary key extracted from said information with the binary key produced using information from the device;
  - preventing the rendering of the information if the binary key associated with the information is not identical to the binary key produced using the device.

44.-54. (CANCELLED)

55. (CURRENTLY AMENDED) The process as set forth in claim 43~~claim 54~~, wherein the encoding of the binary key and the unique physical media identifier is effected by physically altering a portion of the optical medium outside that used to store data representing information to be rendered.

56. (CURRENTLY AMENDED) The process as set forth in claim 55~~claim 54~~ wherein the device comprises a CD-player, a DVD-player or a videodisc player.

57. (ORIGINAL) The process as set forth in claim 55, wherein the binary key is encoded on the surface of the optical medium using a physical structure distinct from that used to encode data representing information to be rendered on said structure.

58. (ORIGINAL) The process as set forth in claim 57, wherein the data as encoded in the physical structure is to be read by a laser at an angle other than 90 degrees.

59. (ORIGINAL) The process as set forth in claim 55, wherein the device detects the binary key and the unique physical media identifier by evaluating a circuit attached to or embedded within the optical medium.

60. (ORIGINAL) The process as set forth in claim 55, wherein the unique physical media identifier and the binary key are stored in a circuit embedded within the optical medium and the device reads the information in said circuit by activating the circuit upon contact with the device.

61. (ORIGINAL) The process as set forth in claim 55, wherein the unique physical media identifier and the binary key are stored in a circuit attached to the spindle hole of the optical medium.

62. (ORIGINAL) The process as set forth in claim 55, wherein the binary key and the unique physical media identifier are encoded in the inner side surface of the spindle hole of the optical medium in a form that may be read by optical or magnetic means located within the device that is to render the encoded information.

63. (ORIGINAL) A process for preventing the unauthorized rendering of a audiovisual or audio work in a digital form, wherein the process comprises:

- producing a binary key using information derived from at least one physical component of a device capable of rendering the work;
- encoding the information representing the audio or audiovisual work using an algorithm in conjunction with the binary key so produced;
- distributing the information to the location at which the information is to be rendered;
- prior to or during the rendering of the information on a device capable of rendering said information,
  - producing a binary key using information derived from at least one physical component of the device;
  - decoding the encoded information using the binary key produced;
  - rendering the decoded information.

64.-66. (CANCELLED)